

10/577005

IAP15 Rec'd PCT/PTO 24 APR 2006


Isabel Leonard  
Medical and Technical Translation  
5 Hearn Street, Watertown, MA 02472-1502, USA  
Phone 617-661-3273 Fax 253-595-9305  
e-mail: isabelleleonard@comcast.net

File 3000-52

### VERIFICATION OF TRANSLATION

I hereby declare and state that I am knowledgeable of each of the German and English languages and that I made and reviewed the attached translation of an International Preliminary Examination Report relating to the patent application entitled "Method of Storing Data in a Random Access Memory, and an Encryption and Decryption Device" from the German language into the English language, and that I believe my attached translation to be accurate, true, and correct to the best of my knowledge and ability.

Date: April 14, 2006

  
\_\_\_\_\_  
Isabel A. Leonard  
Translator

# PATENT COOPERATION TREATY

## PCT

### INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (Chapter II of the Patent Cooperation Treaty)

Applicant or Agent file number: MIF 109WO	<b>FURTHER ACTION</b> See Form PCT/IPEA/416	
International Application No: PCT/EP2004/012435	International filing date: (day/month/year): 03.11.2004	Priority date (day/month/year): 10.11.2003
International Patent Classification (IPC) or national classification and IPC: G06F12/14		
Applicant: MICRONAS GMBH et al.		
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p style="margin-left: 20px;">a. <input type="checkbox"/> (sent to the applicant and to the International Bureau) a total of    sheets, as follows:</p> <p style="margin-left: 40px;"><input type="checkbox"/> sheets of the description, claims, and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p style="margin-left: 40px;"><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p style="margin-left: 20px;">b. <input type="checkbox"/> (sent to the International Bureau only) a total of (indicate type and number of electronic media)    , containing a sequence listing and/or tables related thereto, in electronic form only, as indicated in the Supplemental Box relating to sequence listing (see Section 802 of the Administrative Instructions).</p> <p>4. This report contains indications relating to the following items:</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> Box No. I      Basis of the report</p> <p style="margin-left: 20px;"><input type="checkbox"/> Box No. II     Priority</p> <p style="margin-left: 20px;"><input type="checkbox"/> Box No. III    No opinion with regard to novelty, inventive step, and industrial applicability</p> <p style="margin-left: 20px;"><input type="checkbox"/> Box No. IV    Lack of unity of invention</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> Box No. V     Reasoned statement under Article 35(2) with regard to novelty, inventive step, or industrial applicability; citations and explanations supporting such statement</p> <p style="margin-left: 20px;"><input type="checkbox"/> Box No. VI    Certain documents cited</p> <p style="margin-left: 20px;"><input type="checkbox"/> Box No. VII   Certain defects in the international application</p> <p style="margin-left: 20px;"><input type="checkbox"/> Box No. VIII   Certain observations on the international application</p>		
Date of submission of the demand 10.06.2005	Date of completion of this report 20.01.2006	
Name and address of international preliminary examination authority European Patent Office D-80298 Munich Tel. +49 89 2399-0 Tx: 523656 epmu d Fax: +49 89 2399-4465		Authorized officer  S. Mezödi  Tel. +49 89 2399-6092

**INTERNATIONAL PRELIMINARY REPORT ON  
PATENTABILITY**

International application No.  
PCT/EP2004/012435

---

**Box No. 1 Basis of Report**

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise stated in this item.
- ☐ The report is based on a translation of the international application into the following language, which is the language of a translation furnished for the purposes of:
- ☐ international search (Rules 12.3(a) and 23.1(b))
  - ☐ publication of the international application (Rule 12.4(a))
  - ☐ international preliminary examination (Rules 55.2(a) and/or 55.3(a))
2. With regard to the **elements\*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

**Specification, pages:**

1-23 in the version originally filed

**Claims, Nos.:**

2-10, 12, 13 in the version originally filed

1, 1 received on June 23, 2005 with letter of June 20, 2005

**Drawings, pages:**

1/9-9/9 in the version originally filed

- ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.
3. ☐ The amendments have resulted in the cancellation of the following documents:
- ☐ description, pages
  - ☐ claims, Nos.
  - ☐ drawings, sheets/figs.
  - ☐ sequence listing (*specify exactly*):
  - ☐ any table(s) related to sequence listing (*specify exactly*):
4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
- ☐ description, pages
  - ☐ claims, Nos.
  - ☐ drawings, sheets/figs.
  - ☐ sequence listing (*specify exactly*):
  - ☐ any table(s) related to sequence listing (*specify exactly*):

4\* If item 4 applies, some or all of those sheets may be marked "superseded."

**INTERNATIONAL PRELIMINARY REPORT ON  
PATENTABILITY**

International application No.  
PCT/EP2004/012435

---

**Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step, or industrial applicability; citations and explanations supporting such statement**

**1. Findings**

Novelty (N)	Yes:	Claims 4-9, 12-13
	No:	Claims 1-3, 10, 11
Inventive step (IS)	Yes:	Claims 5, 6, 12, 13
	No:	Claims 1-4, 7-10, 11
Industrial applicability (IA)	Yes:	Claims 1-13
	No:	Claims:

**2. Citations and explanations (Rule 70.7)**

**See attachment**

**Re Item V.**

- 1 In this office action, reference is made to the following documents:  
D1: US-A-5-095 525 (ALMGREN ET AL.) March 10, 1992 (1992-03-10)  
D2: EP-A-1 022 659 (PHILIPS INTELLECTUAL PROPERTY &  
STANDARDS GMBH; KONINKLIJKE PHILIPS EL) July 26, 2000  
(2000-07-26)
- 2 INDEPENDENT CLAIMS 1 AND 11
- 2.1 This application does not meet the requirements of PCT Article 33(1) because the subject matter of Claim 1 is not novel as defined by PCT Article 33(2). Document D2 discloses (references in parentheses refer to this document):

A method of storing data in a random access memory..., in which before storage an encryption of each data word is effected whereby a permuted data word with a predetermined number of data bits is generated from each data word ... by one-to-one permutation of the individual data bits using a first permutation key.  
(Para. 0016, 0017), wherein  
- the first permutation key is generated from a binary random sequence.  
(Para. 0020, a clocked feedback shift register is a (pseudo)-random sequence generator)

- 2.2 This invention does not meet the requirements of PCT Article 33(1) because the subject matter of Claim 1 is not based on an inventive step with reference to D1 as defined by PCT Article 33(3). Document D1 discloses (references in parentheses refer to this document):

A method of storing data in a random access memory..., in which before storage an encryption of each data word is effected whereby a permuted data word with a predetermined number of data bits is generated from each data word ... by one-to-one permutation of the individual data bits using a first permutation key.

(column 6, lines 28 – 41)

The subject matter of Claim 1 therefore differs from the known method by the fact that the first permutation key is generated from a binary random sequence.

It is, however, standard practice in the art to generate keys automatically from random numbers. The individual skilled in the art would include such a feature in the method from D1, and thus arrive at a method according to Claim 1 without any inventive step.

- 2.3 The features of the independent device Claim 11 essentially correspond to those of method Claim 1; accordingly, the above objection also applies to this claim.

### 3 DEPENDENT CLAIMS

Dependent Claims 2-4 and 7-10 do not contain any additional features which, in combination with the features of any claim which they cross-reference, meet the requirements in regard to novelty or an inventive step since what is involved are features either known from D1 or D2 or are standard practice in the art.

Amended Claim 1

1. Method of storing data in a random access memory in which data words, which each comprise a predetermined number of data bits, are storable,  
*characterized in that*

before storage an encryption of each data word (M) is effected whereby a permuted data word (Mp) with a predetermined number of data bits is generated from each data word (M), or from a data word (M) derived from this data word, by one-to-one permutation of the individual data bits (M[n-1]-M[0]) using a first permutation key (P) generated from a binary random sequence.

## Amended Claim 11

11. Device for encrypting/decrypting a data word (M) comprising data bits ( $M[n-1]$ ,  $M[k]$ ,  $M[0]$ ), which device has a permutation unit (14) with the following features:

- data inputs to supply the data bits ( $M[n-1]$ ,  $M[k]$ ,  $M[0]$ ) of the data word to be permuted (M);
- outputs to supply the data bits ( $Mp[n-1]$ ,  $Mp[k]$ ,  $Mp[0]$ ) of a permuted data word (Mp) of the predetermined length (n);
- permutation key inputs to supply a permutation key (P) which comprises a number (n) of subkeys ( $P[n-1]$ ...  $P[0]$ ) corresponding to the number of data bits;
- a signal generator (13) which generates the permutation key (P) from a binary random sequence (RS);
- a number of selection units ( $14\_n-1$ ,  $14\_k$ ,  $14\_0$ ) corresponding to the number of data bits, to which selection units one subkey each is assigned and which each provide one data bit ( $Mp[n-1]$ ,  $Mp[k]$ ,  $Mp[0]$ ) of the permuted data word (Mp) as determined by one each of the subkeys ( $P[n-1]$ ...  $P[0]$ ) from the data bits of the data word to be permuted (M).